MN

Notice of Allowability	Application No.	Applicant(s)	
	10/786,284	ZIMMER ET AL.	
	Examiner	Art Unit	
	Carlton V. Johnson	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *5-11-2007 and phone conversation with Andrew J. Cameron on 8-3-2007*.

2. ☒ The allowed claim(s) is/are *1-20 & 23-28 now renumbered to 1-26*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____.
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

8/6/07

EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Andrew J. Cameron Registration No. 50,281 on August 3, 2007.

The application has been amended as follows:

Claims **11, 20, 26** have been amended as follows:

11. (Currently Amended) A method, comprising:

measuring at least one integrity metric corresponding to a trusted portion of an original firmware configuration of a computer system, wherein the trusted portion of the original firmware configuration includes a startup portion of at least one of system management mode (SMM) firmware code or platform management interrupt (PMI) firmware code;

measuring an unqualified current portion of firmware during an operating system (OS)-runtime phase of the computer system;

storing a respective measurement corresponding to each of said at least one integrity metric in a corresponding platform configuration register (PCR) of a trusted platform module(TPM); and

sealing a secret to the TPM, the secret contained in a digest including the secret concatenated with the respective measurement(s) stored in the PCR(s), wherein a current firmware configuration includes a portion that matches the trusted portion of the original firmware configuration to unseal the secret

attempting to unseal the secret sealed to the TPM during an operating system (OS)- runtime phase of the computer system.

20. (Previously Presented) An article of manufacture, comprising:

a machine-readable medium have instructions stored thereon, which when executed perform operations including:

measuring a trusted portion of an original set of firmware components during a pre-boot phase of a computer system;

storing the measurement of the trusted portion of the original set of firmware components in a trusted platform module (TPM) platform configuration register (PCR);

measuring an unqualified portion of a current set of firmware components during an operating system (OS)-runtime phase of the computer system;

determining if the measurement of the portion of the current set of firmware components matches the measurement of the portion of the original firmware components; and

providing indicia to a processor to execute the portion of the current set of firmware components as a trusted process if the measurements match,
wherein each of the original and current sets of firmware components correspond to a portion of at least one of system management mode (SMM) firmware code or platform management interrupt (PMI) firmware code.

26. (Currently Amended) A system comprising:

a processor, including microcode instructions;
memory, operatively coupled to the processor;
a trusted platform module, operatively coupled to the processor; and
a flash device having firmware instructions stored thereon, which when executed on the processor perform operations including:

retrieving a first measurement stored in the TPM, the first measurement comprising a measurement of a trusted portion of the firmware instructions;

measuring an unqualified current portion of firmware instructions during an operating system (OS)-runtime phase of the system, the current portion of firmware instructions analogous to the trusted portion of the firmware

instructions to obtain a second measurement, wherein each of the trusted and current portions of firmware instructions correspond to a portion of at least one of system management mode (SMM) firmware or platform management interrupt (PMI) firmware;

comparing the first measurement to the second measurement; and
if the first and second measurements match, programming the processor to execute the current portion of firmware instructions as a secure process.

Allowable Subject Matter

The following is an examiner's statement of reasons for allowance:

Claims **1 - 20 and 23 - 28** are allowed.

The current prior art discloses the capability to measure a current portion of firmware during a pre-boot phase of a computer system operation.

However, the current prior art does not disclose a system that is capable of measuring an unqualified current portion of firmware during an operating system (OS)-runtime phase of the computer system. An unqualified portion of firmware is a unmeasured portion of firmware.

So as indicated by the above statements, Applicant's arguments have been considered persuasive, in light of the set of claims with limitations as well as the enabling portions of the specification. The dependent claims further limit the independent claims and are considered allowable on the same basis as the independent claims as well as for the further limitations set forth.

Any comments considered necessary by applicant must be submitted no later

than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carlton V. Johnson whose telephone number is 571-270-1032. The examiner can normally be reached on Monday thru Friday , 8:00 - 5:00PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Carlton V. Johnson
Examiner
Art Unit 2136

CVJ
July 23, 2007

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

8, 6, 07